EXHIBIT A

ORIGINAL

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Gmail Account Jiaqiongxu.udel@gmail.com, Maintained at Premises Controlled by Google, USAO Reference No. 2014R00251

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

15 mag 3209

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF WESTCHESTER)

SALVATORE LOMANTO, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 1986. I am currently assigned to the FBI's White Plains Resident Agency, where I investigate a variety of crimes related to counter-intelligence, including espionage and the theft of trade secrets. During my time as an FBI Special Agent, I have become familiar with some of the ways in which individuals who steal trade secrets and other protected information operate. Through my training and experience, I have become familiar with some of the ways in which such individuals use the Internet, including electronic mail, and have participated in the execution of search warrants involving electronic evidence.

B. The Provider, the Subject Account and the Subject Offense

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the Gmail account Jiaqiongxu.udel@gmail.com (the "Subject Account"), maintained by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("Google"). The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Account contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1832 (theft of trade secrets) (the "Subject Offense"). That statute, in relevant part, provides:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; [or]
>
> (4) attempts to commit any offense described in paragraphs (1) through (3)
>
> [shall be guilty of a crime]

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being

submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

5. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

D. Jurisdiction and Authority to Issue Warrant

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information

pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated."[1] 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. The Subject Account Contains Evidence, Fruits, and Instrumentalities of the Subject Offense

9. As set forth in greater detail below, probable cause exists to believe that the Subject Account contains evidence, fruits, and instrumentalities of the theft of a trade secret. Since in or around November 2014, the FBI has been investigating a particular individual (the "Target") in connection with the theft of computer code for the General Parallel File System ("GPFS") from the International Business Machines Corporation ("IBM"). As part of that investigation, the Target has engaged in recorded conversations and email exchanges with FBI undercover agents ("UC-1" and "UC-2" and, collectively, "the UCs"), during which the Target has discussed the

[1] The Subject Account's apparent user has repeatedly communicated about the Subject Offense with law enforcement officers, at least one of whom was located in the Southern District of New York for at least some of their communications. Moreover, since the Subject Offense appears to have begun and/or is being committed "out of the jurisdiction of any particular State or district," venue over any prosecution is appropriate "in the district in which the offender or any one of two or more joint offenders, is . . . first brought." 18 U.S.C. § 3238.

Target's theft of GPFS code from IBM. The Target has provided the Subject Account as his professional email address and repeatedly used the Subject Account to communicate with the UCs, including, on one occasion, to transmit what appeared to be proprietary portions of GPFS code.

GPFS Background

10. Based on my review of FBI reports, information provided by IBM, open source materials, and my participation in this investigation, I know that GPFS is a clustered file system developed and marketed by IBM. IBM produces this code for use in high-performance computer systems. Customers include government agencies and private corporations. According to IBM's public website, GPFS "powers many of the world's largest scientific supercomputers and commercial applications requiring high-speed access to large volumes of data." Industries that use GPFS include digital media, engineering, design, business intelligence, financial analytics, seismic data processing, geographic information systems, and scalable file serving. The source code underlying GPFS (the "GPFS Code")—that is, the computer instructions or commands that comprise the software—is proprietary information, which IBM does not sell to customers.

Target Background

11. From my review of FBI reports and information obtained from IBM, I know that the Target worked for IBM China from November 2010 to May 2014. At the outset of the Target's IBM employment, the Target signed a document entitled "Agreement Regarding Confidential Information and Intellectual Property," which provided, among other things, that the Target would not disclose "any confidential information or material of IBM or its affiliates." At IBM China, the Target worked as a developer and had full access to the GPFS Code, including the

ability to download the GPFS Code to a computer or digital storage device. In May 2014, the Target voluntarily resigned from IBM.

November 2014-March 2015: Subject Account Used to Discuss and Share the GPFS Code

12. From my review of FBI reports, I know that in or around fall 2014, the FBI received a report that someone other than the Target had contacted a particular individual ("Individual-1"), informed Individual-1 that the Target had access to the GPFS Code, and indicated to Individual-1 that the Target was using the GPFS Code in business ventures that were not related to IBM clients.

13. In or around November 2014, UC-1 contacted the Target via email. For purposes of this investigation, UC-1 posed as a financial investor aiming to start a large data storage-oriented technology company. I have reviewed copies of emails that UC-1 exchanged with the Target between November 2014 and March 2015. From my review of those emails, I have learned the following:

a. On or about November 27, 2014, UC-1 emailed the Target at an address other than the Subject Account. UC-1 indicated that Individual-1 had mentioned the Target as someone who could be helpful to UC-1's startup company.

b. On or about November 27, 2014, the Target replied to UC-1 using the Subject Account. Among other things, the Target indicated that he had "several years working experience over this field and spent most of my career in IBM working on the development of GPFS which is a large-scale parallel storage system used in lots of hyper-scale cluster systems in the world." The Target also expressed interest in discussing UC-1's project, as well as "further opportunities."

c. On or about November 29, 2014, UC-1 responded to the Target, and expressed interest in communicating further at some point in mid-December.

d. On or about December 3, 2014, the Target responded, using the Subject Account, and provided times when the Target would be available to communicate via Skype[2] or similar digital communications services.

e. On or about January 8, 2015, the Target again emailed UC-1, using an account other than the Subject Account. The Target indicated that the Target had previously sent UC-1 two emails from the Subject Account but was unsure if UC-1 had received them. The Target expressed the Target's continued interest in collaboration with UC-1.

f. On or about February 18, 2015, UC-1 replied to the Target, at an address other than the Subject Account, apologized for the delay in responding, and encouraged the Target to send UC-1 a resume if the Target remained interested in working with UC-1. On or about February 19, 2015, UC-1 forwarded that message to the Subject Account.

g. On or about February 19, 2015, the Target responded to UC-1 from the Subject Account and included a copy of the Target's resume (the "Resume"). Among other things, the Resume listed the Subject Account as the Target's email address and noted that the Target had worked on GPFS at IBM.

h. On or about March 16, 2015, the Target sent an email to UC-1 and UC-2[3] ("the GPFS Code Email") from the Subject Account. In the GPFS Code Email, the Target described some of the Target's previous work with GPFS and reported that he had "attached some sample code of [his] previous work in IBM." The Target also pasted a "short GPFS+NFS related patch" directly into the GPFS Code Email, purportedly for the purpose of showing his "coding style."

---

[2] Based on my training and experience, I know that Skype is a mode of Internet communication, which allows for text-based messaging, as well as digital voice and, potentially, video communication.

[3] For purposes of this investigation, UC-2 was posing as a project manager, working for UC-1.

14. From my review of FBI reports, I know that FBI agents showed the computer code that the Target emailed to the UCs, see supra ¶ 13(h), to an IBM employee (the "IBM Employee"), who is intimately familiar with GPFS. The IBM Employee confirmed that the GPFS Code Email included proprietary material that related to the GPFS Code.

April-May 2015: The Target Discusses Theft of GPFS Code

15. Between on or about April 7, 2015, and on or about April 9, 2015, the Target sent UC-2 three email messages regarding the scheduling of a Skype conversation to discuss "project collaboration" (the "Scheduling Messages"). From my review of the Scheduling Messages, I know that all of the Scheduling Messages were sent from the Subject Account. The last of the Scheduling Messages confirmed that the conversation would take place on April 12, 2015.

16. On or about April 12, 2015, UC-2 participated in a recorded audio Skype conversation with the Target. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of the draft transcript, I have learned the following, in substance and in part:

a. The Target stated that the Target had "all the GPFS code."

b. At one point UC-2 inquired as to whether the Target "was allowed to have this code, since it's IBM's" and clarified that UC-2 was asking if UC-2 should "be a little . . . discreet as to who [UC-2] show[ed] it to." The Target replied that "Yes, we signed some, you know, signed some files there but actually I can, um, I can, I, I have all the code." Based on my training, experience, and participation in this investigation, it appears that the Target's reference to having "signed some files" was an acknowledgement that the Target had signed a non-disclosure agreement as part of the Target's IBM employment, see supra ¶ 11.[4]

c. The Target made reference to the fact that, in his experience, start-up companies often used code obtained from large, established companies, "because no one, ah, no one want to, you know, code from the, the first line." Based on my training, experience, and participation in this investigation, it appears that the Target was intimating to UC-2 that the Target could provide the GPFS Code to UC-2 to accelerate the development of UC-2's company's product.

d. The Target reported that the Target had already used a portion of the GPFS Code as part of the Target's then-current employment at a technology startup company.

17. On or about May 11, 2015, UC-2 participated in a recorded audio Skype conversation with the Target. I have reviewed a draft transcript of that conversation, which was conducted in English. From my review of that transcript, I have learned that the Target said the following, in substance and in part:

a. The Target again stated that the Target had used "some of the [GPFS] code" in the Target's work after the Target left IBM.

b. The Target stated that the Target was willing to consider providing UC-2's company with the GPFS Code as a platform for UC-2's company to facilitate the development of UC-2's company's own data storage system.

---

[4] In addition to the non-disclosure agreement, see supra ¶ 11, the Target may also have been referring to an exit affidavit that he completed before leaving IBM's employment. I have reviewed an IBM document with the header "Affidavit," which appears to have been completed by the Target in Mandarin—which I do not speak—in connection with the conclusion of the Target's employment by IBM. Among other things, that document bears the Target's identification card number. It also reads, in part, in English "I hereby represent that I have settled/returned or will settle/return all debit/assets due IBM."

c. The Target informed UC-2 that if UC-2 set up several computers as a small network, then the Target would remotely install the GPFS Code so that the UCs could test it and confirm its functionality.

18. On or about June 1, 2015, UC-2 emailed the Target at the Subject Account, to confirm that the UCs would set up several computers per the Target's specifications. On or about June 2, 2015, UC-2 received a response from the Subject Account, in which the Target stated, among other things that he "ha[d] a lot of thinking about what we can do in storage layer to better support the big-data applications."

19. From my review of FBI reports, I know that in or around early August 2015, the Target remotely uploaded files to several computers that the FBI had made available to the Target for that purpose. Based on preliminary assessment of those files by the IBM Employee, those files appear to contain portions of GPFS and other proprietary IBM files.

20. On or about May 7, 2015, a preservation request was served on Google, pursuant to 18 U.S.C. § 2703(f), to ensure that the Subject Account's contents would be preserved. On or about September 2, 2015, a second such preservation request was served on Google.

Request to Search the Subject Account

21. Based on my training and experience, I have learned that:

a. Email accounts are typically used as long-term repositories for old emails, such that the GPFS Code Email and the Scheduling Messages will likely still be in the Subject Account when we search it.

b. Criminals make repeated use of those email accounts they believe are trusted and secure for their illegal dealings—such that if an individual uses a particular email account as part of a particular course of criminal conduct (as, for example, the Target appears to have used the

Subject Account), there is probable cause to believe that that email account contains other information related to that course of criminal conduct.

c. The above two inferences are greatly strengthened when, as here, (i) the investigation involves international criminals, who need to communicate with people quickly, cheaply, and securely across borders, and (ii) the international criminal has already made use of email in direct furtherance of the Subject Offense.

22. Based on the foregoing, there is probable cause to believe the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offense. Specifically, I believe there is probable cause to believe that the Subject Account is likely to contain:

a. Stored email communications and other stored content information presently contained in, or on behalf of, the account in question;

b. Transactional information of activity on the account described above, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations; and

c. Contact lists, address books, calendars, photographs, appointment lists, and other such related content.

23. Further, based on my training and experience, I respectfully submit that there is probable cause to believe that the information described above will contain evidence, fruits, and instrumentalities of violations of federal law, including but not limited to the Subject Offense, including but not limited to email correspondence regarding:

a. Communications concerning the illicit acquisition, retention, and/or sale of the GPFS Code and other proprietary computer code;

b. Communications concerning the origin, destination, and distribution of the GPFS Code and other proprietary computer code;

c. Records of negotiations regarding the prices or sale of the GPFS Code and other proprietary computer code;

d. Conversations concerning illicit financial transactions (e.g. payment for trade secrets), including but not limited to conversations regarding bank accounts;

f. Communications showing the identity and/or location of individual(s) using the Subject Account or accounts used to communicate with the Subject Account; and

g. Identifying information pertaining to the Target, including but not limited to names, residences, locations, telephone numbers, PINs, email addresses, social security numbers, nationalities, and passport information.

24. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offense, as more fully described in Section II of Attachment A to the proposed warrant.

Review of the Information Obtained Pursuant to the Warrant

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, and outside technical experts under government control) will retain the

records and review them for evidence, fruits, and instrumentalities of the Subject Offense as specified in Section III of Attachment A to the proposed warrant.

26. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offense, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords for which an agent is likely to search.

27. When conducting the searches authorized by the proposed warrant, law enforcement personnel will make reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information which are identified in the proposed warrant themselves.

III. Request for Non-Disclosure and Sealing Order

28. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert

potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. This is a particularly salient concern here, since the Target remains at liberty and has a demonstrated fluency in digital technology.

29. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

30. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

IV. Conclusion

31. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

SALVATORE LOMANTO
Special Agent
Federal Bureau of Investigation

Sworn to before me this
9th day of September, 2015

HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of a Warrant for All Content and Other Information Associated with the Gmail Account Jiaqiangxu.udel@gmail.com, Maintained at Premises Controlled by Google, USAO Reference No. 2014R00251

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

15 mag 3255

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF WESTCHESTER)

SALVATORE LOMANTO, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 1986. I am currently assigned to the FBI's White Plains Resident Agency, where I investigate a variety of crimes related to counter-intelligence, including espionage and the theft of trade secrets. During my time as an FBI Special Agent, I have become familiar with some of the ways in which individuals who steal trade secrets and other protected information operate. Through my training and experience, I have become familiar with some of the ways in which such individuals use the Internet, including electronic mail, and have participated in the execution of search warrants involving electronic evidence.

B. The Provider, the Subject Account and the Subject Offense

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for all content and other information associated with the Gmail account Jiaqiangxu.udel@gmail.com (the "Subject Account"), maintained by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 ("Google"). The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant.

3. As detailed below, there is probable cause to believe that the Subject Account contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1832 (theft of trade secrets) (the "Subject Offense"). That statute, in relevant part, provides:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; [or]
>
> (4) attempts to commit any offense described in paragraphs (1) through (3)
>
> [shall be guilty of a crime]

4. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I

have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of the Provider

5. Based on my training, experience, and participation in this investigation, I know the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

iv. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

v. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

vi. *Preserved records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

D. Jurisdiction and Authority to Issue Warrant

6. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated."[1] 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. The Subject Account Contains Evidence, Fruits, and Instrumentalities of the Subject Offense

9. As set forth in greater detail below, probable cause exists to believe that the Subject Account contains evidence, fruits, and instrumentalities of the theft of a trade secret. Since in or around November 2014, the FBI has been investigating a particular individual (the "Target") in connection with the theft of computer code for the General Parallel File System ("GPFS") from the International Business Machines Corporation ("IBM"). As part of that investigation, the Target has engaged in recorded conversations and email exchanges with FBI undercover agents ("UC-1" and "UC-2" and, collectively, "the UCs"), during which the Target has discussed the Target's theft of GPFS code from IBM. The Target has provided the Subject Account as his professional email address and repeatedly used the Subject Account to communicate with the

[1] The Subject Account's apparent user has repeatedly communicated about the Subject Offense with law enforcement officers, at least one of whom was located in the Southern District of New York for at least some of their communications. Moreover, since the Subject Offense appears to have begun and/or is being committed "out of the jurisdiction of any particular State or district," venue over any prosecution is appropriate "in the district in which the offender or any one of two or more joint offenders, is . . . first brought." 18 U.S.C. § 3238.

UCs, including, on one occasion, to transmit what appeared to be proprietary portions of GPFS code.

GPFS Background

10. Based on my review of FBI reports, information provided by IBM, open source materials, and my participation in this investigation, I know that GPFS is a clustered file system developed and marketed by IBM. IBM produces this code for use in high-performance computer systems. Customers include government agencies and private corporations. According to IBM's public website, GPFS "powers many of the world's largest scientific supercomputers and commercial applications requiring high-speed access to large volumes of data." Industries that use GPFS include digital media, engineering, design, business intelligence, financial analytics, seismic data processing, geographic information systems, and scalable file serving. The source code underlying GPFS (the "GPFS Code")—that is, the computer instructions or commands that comprise the software—is proprietary information, which IBM does not sell to customers.

Target Background

11. From my review of FBI reports and information obtained from IBM, I know that the Target worked for IBM China from November 2010 to May 2014. At the outset of the Target's IBM employment, the Target signed a document entitled "Agreement Regarding Confidential Information and Intellectual Property," which provided, among other things, that the Target would not disclose "any confidential information or material of IBM or its affiliates." At IBM China, the Target worked as a developer and had full access to the GPFS Code, including the ability to download the GPFS Code to a computer or digital storage device. In May 2014, the Target voluntarily resigned from IBM.

November 2014-March 2015: Subject Account Used to Discuss and Share the GPFS Code

12. From my review of FBI reports, I know that in or around fall 2014, the FBI received a report that someone other than the Target had contacted a particular individual ("Individual-1"), informed Individual-1 that the Target had access to the GPFS Code, and indicated to Individual-1 that the Target was using the GPFS Code in business ventures that were not related to IBM clients.

13. In or around November 2014, UC-1 contacted the Target via email. For purposes of this investigation, UC-1 posed as a financial investor aiming to start a large data storage-oriented technology company. I have reviewed copies of emails that UC-1 exchanged with the Target between November 2014 and March 2015. From my review of those emails, I have learned the following:

a. On or about November 27, 2014, UC-1 emailed the Target at an address other than the Subject Account. UC-1 indicated that Individual-1 had mentioned the Target as someone who could be helpful to UC-1's startup company.

b. On or about November 27, 2014, the Target replied to UC-1 using the Subject Account. Among other things, the Target indicated that he had "several years working experience over this field and spent most of my career in IBM working on the development of GPFS which is a large-scale parallel storage system used in lots of hyper-scale cluster systems in the world." The Target also expressed interest in discussing UC-1's project, as well as "further opportunities."

c. On or about November 29, 2014, UC-1 responded to the Target, and expressed interest in communicating further at some point in mid-December.

d. On or about December 3, 2014, the Target responded, using the Subject Account, and provided times when the Target would be available to communicate via Skype[2] or similar digital communications services.

e. On or about January 8, 2015, the Target again emailed UC-1, using an account other than the Subject Account. The Target indicated that the Target had previously sent UC-1 two emails from the Subject Account but was unsure if UC-1 had received them. The Target expressed the Target's continued interest in collaboration with UC-1.

f. On or about February 18, 2015, UC-1 replied to the Target, at an address other than the Subject Account, apologized for the delay in responding, and encouraged the Target to send UC-1 a resume if the Target remained interested in working with UC-1. On or about February 19, 2015, UC-1 forwarded that message to the Subject Account.

g. On or about February 19, 2015, the Target responded to UC-1 from the Subject Account and included a copy of the Target's resume (the "Resume"). Among other things, the Resume listed the Subject Account as the Target's email address and noted that the Target had worked on GPFS at IBM.

h. On or about March 16, 2015, the Target sent an email to UC-1 and UC-2[3] ("the GPFS Code Email") from the Subject Account. In the GPFS Code Email, the Target described some of the Target's previous work with GPFS and reported that he had "attached some sample code of [his] previous work in IBM." The Target also pasted a "short GPFS+NFS related patch" directly into the GPFS Code Email, purportedly for the purpose of showing his "coding style."

---

[2] Based on my training and experience, I know that Skype is a mode of Internet communication, which allows for text-based messaging, as well as digital voice and, potentially, video communication.

[3] For purposes of this investigation, UC-2 was posing as a project manager, working for UC-1.

14. From my review of FBI reports, I know that FBI agents showed the computer code that the Target emailed to the UCs, see supra ¶ 13(h), to an IBM employee (the "IBM Employee"), who is intimately familiar with GPFS. The IBM Employee confirmed that the GPFS Code Email included proprietary material that related to the GPFS Code.

April-May 2015: The Target Discusses Theft of GPFS Code

15. Between on or about April 7, 2015, and on or about April 9, 2015, the Target sent UC-2 three email messages regarding the scheduling of a Skype conversation to discuss "project collaboration" (the "Scheduling Messages"). From my review of the Scheduling Messages, I know that all of the Scheduling Messages were sent from the Subject Account. The last of the Scheduling Messages confirmed that the conversation would take place on April 12, 2015.

16. On or about April 12, 2015, UC-2 participated in a recorded audio Skype conversation with the Target. I have reviewed that recording, as well as a draft transcript of that conversation, which was conducted in English. From my review of the draft transcript, I have learned the following, in substance and in part:

a. The Target stated that the Target had "all the GPFS code."

b. At one point UC-2 inquired as to whether the Target "was allowed to have this code, since it's IBM's" and clarified that UC-2 was asking if UC-2 should "be a little . . . discreet as to who [UC-2] show[ed] it to." The Target replied that "Yes, we signed some, you know, signed some files there but actually I can, um, I can, I, I have all the code." Based on my training, experience, and participation in this investigation, it appears that the Target's reference to having "signed some files" was an acknowledgement that the Target had signed a non-disclosure agreement as part of the Target's IBM employment, see supra ¶ 11.[4]

c. The Target made reference to the fact that, in his experience, start-up companies often used code obtained from large, established companies, "because no one, ah, no one want to, you know, code from the, the first line." Based on my training, experience, and participation in this investigation, it appears that the Target was intimating to UC-2 that the Target could provide the GPFS Code to UC-2 to accelerate the development of UC-2's company's product.

d. The Target reported that the Target had already used a portion of the GPFS Code as part of the Target's then-current employment at a technology startup company.

17. On or about May 11, 2015, UC-2 participated in a recorded audio Skype conversation with the Target. I have reviewed a draft transcript of that conversation, which was conducted in English. From my review of that transcript, I have learned that the Target said the following, in substance and in part:

a. The Target again stated that the Target had used "some of the [GPFS] code" in the Target's work after the Target left IBM.

b. The Target stated that the Target was willing to consider providing UC-2's company with the GPFS Code as a platform for UC-2's company to facilitate the development of UC-2's company's own data storage system.

---

[4] In addition to the non-disclosure agreement, see supra ¶ 11, the Target may also have been referring to an exit affidavit that he completed before leaving IBM's employment. I have reviewed an IBM document with the header "Affidavit," which appears to have been completed by the Target in Mandarin—which I do not speak—in connection with the conclusion of the Target's employment by IBM. Among other things, that document bears the Target's identification card number. It also reads, in part, in English "I hereby represent that I have settled/returned or will settle/return all debit/assets due IBM."

c. The Target informed UC-2 that if UC-2 set up several computers as a small network, then the Target would remotely install the GPFS Code so that the UCs could test it and confirm its functionality.

18. On or about June 1, 2015, UC-2 emailed the Target at the Subject Account, to confirm that the UCs would set up several computers per the Target's specifications. On or about June 2, 2015, UC-2 received a response from the Subject Account, in which the Target stated, among other things that he "ha[d] a lot of thinking about what we can do in storage layer to better support the big-data applications."

19. From my review of FBI reports, I know that in or around early August 2015, the Target remotely uploaded files to several computers that the FBI had made available to the Target for that purpose. Based on preliminary assessment of those files by the IBM Employee, those files appear to contain portions of GPFS and other proprietary IBM files.

20. On or about May 7, 2015, a preservation request was served on Google, pursuant to 18 U.S.C. § 2703(f), to ensure that the Subject Account's contents would be preserved. On or about September 2, 2015, a second such preservation request was served on Google.

Request to Search the Subject Account

21. Based on my training and experience, I have learned that:

a. Email accounts are typically used as long-term repositories for old emails, such that the GPFS Code Email and the Scheduling Messages will likely still be in the Subject Account when we search it.

b. Criminals make repeated use of those email accounts they believe are trusted and secure for their illegal dealings—such that if an individual uses a particular email account as part of a particular course of criminal conduct (as, for example, the Target appears to have used the

Subject Account), there is probable cause to believe that that email account contains other information related to that course of criminal conduct.

c. The above two inferences are greatly strengthened when, as here, (i) the investigation involves international criminals, who need to communicate with people quickly, cheaply, and securely across borders, and (ii) the international criminal has already made use of email in direct furtherance of the Subject Offense.

22. Based on the foregoing, there is probable cause to believe the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offense. Specifically, I believe there is probable cause to believe that the Subject Account is likely to contain:

a. Stored email communications and other stored content information presently contained in, or on behalf of, the account in question;

b. Transactional information of activity on the account described above, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations; and

c. Contact lists, address books, calendars, photographs, appointment lists, and other such related content.

23. Further, based on my training and experience, I respectfully submit that there is probable cause to believe that the information described above will contain evidence, fruits, and instrumentalities of violations of federal law, including but not limited to the Subject Offense, including but not limited to email correspondence regarding:

a. Communications concerning the illicit acquisition, retention, and/or sale of the GPFS Code and other proprietary computer code;

b. Communications concerning the origin, destination, and distribution of the GPFS Code and other proprietary computer code;

c. Records of negotiations regarding the prices or sale of the GPFS Code and other proprietary computer code;

d. Conversations concerning illicit financial transactions (e.g. payment for trade secrets), including but not limited to conversations regarding bank accounts;

f. Communications showing the identity and/or location of individual(s) using the Subject Account or accounts used to communicate with the Subject Account; and

g. Identifying information pertaining to the Target, including but not limited to names, residences, locations, telephone numbers, PINs, email addresses, social security numbers, nationalities, and passport information.

24. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the Subject Account will contain evidence, fruits, and instrumentalities of the Subject Offense, as more fully described in Section II of Attachment A to the proposed warrant.

Review of the Information Obtained Pursuant to the Warrant

25. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 10 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, and outside technical experts under government control) will retain the

records and review them for evidence, fruits, and instrumentalities of the Subject Offense as specified in Section III of Attachment A to the proposed warrant.

26. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offense, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords for which an agent is likely to search.

27. When conducting the searches authorized by the proposed warrant, law enforcement personnel will make reasonable efforts to utilize computer search methodology to search only for files, documents, or other electronically stored information which are identified in the proposed warrant themselves.

III. Request for Non-Disclosure and Sealing Order

28. The existence and scope of this ongoing criminal investigation is not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert

potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, given that targets of the investigation are known to use computers and electronic communications in furtherance of their activity, the targets could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation. This is a particularly salient concern here, since the Target remains at liberty and has a demonstrated fluency in digital technology.

29. Accordingly, there is reason to believe that, were the Provider to notify the subscribers or others of the existence of the warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

30. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

IV. Prior Application and Conclusion

31. On September 9, 2015, the Honorable Judith C. McCarthy authorized a search of an e-mail account based on the precise facts articulated above (the "Initial Application"). However, the Initial Application contained a typographical error with respect to the Subject Account. Specifically, the Initial Application indicated that the Subject Account was

"Jiaqiongxu.udel@gmail.com," rather than "Jiaqiangxu.udel@gmail.com," that is, it erroneously substituted an "o" for the second "a" in the Subject Account. The typographical error was detected shortly after the search warrant was served, and the FBI will promptly notify the service provider not to make production in response to the initial errant search warrant, but rather only to the search warrant sought herein.

32. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

SALVATORE LOMANTO
Special Agent
Federal Bureau of Investigation

Sworn to before me this
11th day of September, 2015

HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York

Gmail Search Warrant Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Google (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, and applies to all content and other information within the Provider's possession, custody, or control associated with the email account Jiaqiangxu.udel@gmail.com (the "Subject Account").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Account:

a. *Email content.* All emails sent to or from, stored in draft form in, or otherwise associated with the Subject Account, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email);

b. *Address book information.* All address book, contact list, or similar information associated with the Subject Account.

c. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Account, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

d. *Transactional records.* All transactional records associated with the Subject Account, including any IP logs or other records of session times and durations.

e. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Account, including complaints, inquiries, or other contacts with support services and records of actions taken.

f. *Preserved records.* Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1832 (theft of trade secrets), including the following:

a. Communications concerning the illicit acquisition, retention, and/or sale of proprietary computer code;

b. Communications concerning the origin, destination, and distribution of proprietary computer code;

c. Records of negotiations regarding the prices or sale of proprietary computer code;

d. Conversations concerning illicit financial transactions (e.g. payment for trade secrets), including but not limited to conversations regarding bank accounts;

f. Communications showing the identity and/or location of individual(s) using the Subject Account or accounts used to communicate with the Subject Account; and

g. Identifying information pertaining to the Target, including but not limited to names, residences, locations, telephone numbers, PINs, email addresses, social security numbers, nationalities, and passport information.